



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/729,209	12/05/2003	Jean-Pierre Duplessis	MS306247.01/MSFTP552US	9483

27195 7590 01/18/2007
AMIN. TUROCY & CALVIN, LLP
24TH FLOOR, NATIONAL CITY CENTER
1900 EAST NINTH STREET
CLEVELAND, OH 44114

EXAMINER

TRAORE, FATOUMATA

ART UNIT	PAPER NUMBER
----------	--------------

2112

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/18/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/729,209	DUPLESSIS ET AL.	
	Examiner	Art Unit	
	Fatoumata Traore	2112	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 05 December 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-22 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-22 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 12/05/03 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date <u>05/13/04</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

This action is in response of the original filing of December 5, 2003. Claims 1-22 are pending and have been considered below.

Claim Objections

1. Claims 11, 14, and 18 are objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claims, or amend the claims to place the claims in proper dependent form, or rewrite the claims in independent form. Claim 11, 14, and, 18 are improperly dependent on claim 1, 12, and 15 because: the examiner notes that the applicant is claiming the intended used of the system in claim 11, and a computer program in claims 14 and 18 which fail to add, delete, or change any of the steps in the parent claim.
2. Claims 12, 13, 16, and 17 are objected because of the following informalities: the examiner notes the use of acronyms (Wi-fi, EAPOL) throughout the claims without first including a description in plain text, as required.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

The applicant appears to be attempting to invoke 35 U.S.C. 112 6th paragraph in claim 22 by using "means-plus-function" language. However, the Examiner notes that the only "means" for performing these cited functions in the specification appears to be computer programs modules. While the claims pass the first test of the three-prong test used to determine invocation of paragraph 6, since no other specific structural limitations are disclosed in the specification, the claims do not meet the other tests of the three-prong test. Therefore, 35 U.S.C. 112 6th paragraph has not been invoked when considering these claims below.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

Art Unit: 2112

4. Claims 1-6, 8, 9, 11, 12, 21, 22 are rejected under 35 U.S.C. 102(e) as being anticipated by **Tsui** (US 20050063338).

Claims 1-3, 21, and 22: **Tsui** discloses a seamless roaming apparatus, systems, and methods comprising:

- i. A connection component that can connect a device to a plurality of wireless networks (to assist in providing high quality connection) (page 1, paragraph 8); and;
- ii. A detection component that identifies a type of an available wireless network (by detecting available network type) (page 1, paragraph 8).

Claim 2: **Tsui** discloses the seamless roaming apparatus, systems, and methods as in claim 1 above, and further discloses that the identification by the detection component is based, at least in part, upon receipt of an information element from a wireless network beacon. (A beacon detection circuit and software processing to detect the type of network that is available) (page 1, paragraph 12).

Claim 3: **Tsui** discloses the seamless roaming apparatus, systems, and methods as in claim 1 above, and further discloses that the wireless network comprise at least one of an unencrypted network, a wired equivalent Privacy (WEP) network requiring a WEP key, a Wi-Fi Protected Access (WPA) encrypted network requiring a WPA pre-shared key, an

Art Unit: 2112

802.1x-enabled network that does not support WPA, an 802.1x enabled network that does support WPA and a wireless provisioning services (WPS) support-enabled network (the wireless computing platform move from connecting to a first network to a second network) (page 1 paragraph 9).

Claim 11: Tsui discloses a secure Wi-Fi communication system and method to enable automatic network roaming as in claim 1 above. It is inherent that the plurality of networks is run by a plurality of servers. Thus Tsui 's device, which is connecting to the networks, would be considered to be a client system.

5. Claims 4-10, 12, 14, 19, 20 are rejected under 35 U.S.C. 102(e) as being anticipated by Fascenda (US 20040068653).

Claim 4: Fascenda discloses a secure Wi-fi commutation system and method to enable automatic network roaming comprising:

A connection component that can connect a device to a plurality of wireless networks (most access points have an integrated Ethernet controller to connect to an existing wired-Ethernet network) (page 1, paragraph 6); and; A detection component that identifies a type of an available wireless network (Each network identifies itself using the beacon frame) (page 1, paragraph 10) and further discloses that the identification by the detection component being based, at least in part, upon iterative probing of the available network (the client devices detects the presence of the network by listening for a probe request) (page 8, paragraph 69).

Claim 5: **Fascenda** discloses a secure Wi-fi commutation system and method to enable automatic network roaming as in claim 4 above, wherein the detection component attempts to connect to the wireless network as a wireless provisioning service-supporting network, the detection component determine that the network is a pre-shared key network if a failure in an authentication sequence from the wireless network beacon is determine (Even thought the secure mode enabled network appears to all potential users to be wide open , a user can connect to that network without having the proper respective network cryptographic keys. the authentication process discriminates between those users who have valid cryptographic keys and those who do not) (page 6, paragraph 57).

Claim 6: **Fascenda** discloses a secure Wi-Fi commutation system and method to enable automatic network roaming as in claim 5 above, and further discloses identifies the network as a Wi-Fi protected Access network if a failure in a particular piece of authentication (if the network is not secure mode enabled, the computing device attempts to connect to it using standard Wi-Fi parameters) (page 4, paragraph 44).

Claim 7: **Fascenda** discloses a secure Wi-fi commutation system and method to enable automatic network roaming as in claim 6 above, and further disclose that a particular piece of authentication sequence comprise a type of length value sequence

Art Unit: 2112

(Each authentication frame comprises an authentication algorithm number preferably set to an integer number undefined in the 802.11 specification) (page 8, paragraph 68).

Claim 8: **Fascenda** discloses a secure Wi-fi commutation system and method to enable automatic network roaming as in claim 6 above, further identifies the type of the network if a particular piece of authentication sequence is received from the wireless network beacon (the beacon response frame comprises a Basic Service Set Identifier field that uniquely identifies the network and access point and distinguishes the current access point from other access point) (page 8, paragraph 69).

Claim 9: **Fascenda** discloses a secure Wi-fi commutation system and method to enable automatic network roaming comprising:

A connection component that can connect a device to a plurality of wireless networks (most access points have an integrated Ethernet controller to connect to an existing wired-Ethernet network) (page 1, paragraph 6); and; A detection component that identifies a type of an available wireless network (Each network identifies itself using the beacon frame) (page 1, paragraph 10). Wherein the detection component sends at least one of a connect message, an 802.1x EAPOL start message (a list of all Service Set Identifier currently available is displayed to the user, from which the user makes a choice which is also known as a passive mode (page 1, paragraph 11).

Art Unit: 2112

Claim 10: **Fascenda** discloses a secure Wi-fi commutation system and method to enable automatic network roaming comprising:

A connection component that can connect a device to a plurality of wireless networks (most access points have an integrated Ethernet controller to connect to an existing wired-Ethernet network) (page 1, paragraph 6); and; A detection component that identifies a type of an available wireless network (Each network identifies itself using the beacon frame) (page 1, paragraph 10). Wherein the detection component receives at least one of an associated message, an 802.1x identify request message, an authentication message and provisioning message from a wireless network beacon (an alternative method of seeking wireless networks is know as active mode, whereby the Network Interface Card issues a probe request to cause all listening access points within range to respond with an identification frame containing their Service Set Identifier (page 1, paragraph 11).

Claim 12: **Fascenda** discloses a secure Wi-fi commutation system and method to enable automatic network roaming comprising:

- a. Attempting to connect to a wireless network as a wireless provisioning services supporting network (the computer device examines whether a Wi-Fi network exists and if found attempts to authenticate itself with the network) (Page4, paragraph 44);
- b. Determining whether the attempt was successful (if the network is enabled to operate in secure mode) (Page 4, paragraph 44); and;

Art Unit: 2112

- c. Prompting for a wired equivalent privacy key, if the attempt was not successful (if the network is not in secure mode enabled, the computing device attempts to connect using standard WI-Fi parameters (Page1, paragraph 44);

Claim 14: **Fascenda** discloses a secure Wi-Fi communication system and method to enable automatic network roaming as in claim 12 above, and further discloses the connecting devices to be computers (Fig 1). It is inherent that these computers have computer instructions for performing the functions of claim 12 stored thereon.

Claim 19: **Fascenda** discloses a secure Wi-fi commutation system and method to enable automatic network roaming comprising: a data field comprising information identifying a type of wireless network connection based, at least in part, upon iterative probing of available network (the client devices detects the presence of the network by listening for a probe request) (page 8, paragraph 69).

Claim 20: **Fascenda** discloses a secure Wi-Fi communication system and method to enable automatic network roaming, and further discloses that the format of the authentication frames follow a standard 802.11 authentication framing format, the implementation of which is apparent to one ordinary skill in the art (page 8, paragraph 68).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 13, 15-18, 20, are rejected under 35 U.S.C. 103(a) as being unpatentable over **Fascenda** (US 20040068653).

Claim 13: **Fascenda** discloses a secure Wi-Fi communication system and method to enable automatic network roaming as in claim 12 above, and further discloses that the computing device examines whether a Wi-Fi exists and if found, attempts to authenticate itself with that network. If the network is enabled to operate in secure, all of currently configured wireless settings of the computing device are switched to secure mode and the login process is completely automated. If the network is not secure mode enabled, the computing device attempts to connect to it using standard Wi-Fi parameters (page 4, paragraph 0041). Fascenda does not mention distinguishing different type of network. However, to connect to a wireless network one must know the network protocol. In order to do that one need to determine first the network type. One ordinary skilled in the art of programming would attempt to determine the network type in order to connect using the appropriate protocol. Therefore it would have been obvious to distinguish the different type of network before connecting. One would be motivated to do so in order to reduce the time spent by users in attempting to determine the type of such network.

Art Unit: 2112

Claim 15: **Fascenda** discloses a secure Wi-fi commutation system and method to enable automatic network roaming. However, to connect to a wireless network one must know the network protocol. In order to do so, one needs to determine first the network type. One ordinary skilled in the art of programming would attempt to determine the network type in order to connect using the appropriate protocol. Therefore it would have been obvious to distinguish the different type of network before connecting. One would be motivated to do so in order to reduce the time spent by users in attempting to determine the type of such network.

Claim 16: **Fascenda** discloses a secure Wi-Fi communication system and method to enable automatic network roaming as in claim 15 above, Fascenda does not mention distinguishing different type of network. However, to connect to a wireless network one must know the network protocol. In order to do so, one needs to determine first the network type. One ordinary skilled in the art of programming would attempt to determine the network type in order to connect using the appropriate protocol. Therefore it would have been obvious to distinguish the different type of network before connecting. One would be motivated to do so in order to reduce the time spent by users in attempting to determine the type of such network.

Claim 17: **Fascenda** discloses a secure Wi-Fi communication system and method to enable automatic network roaming as in claim 16 above, Fascenda does not mention distinguishing different type of network. However, to connect to a wireless network one

Art Unit: 2112

must know the network protocol. In order to do so, one needs to determine first the network type. One ordinary skilled in the art of programming would attempt to determine the network type in order to connect using the appropriate protocol. Therefore it would have been obvious to distinguish the different type of network before connecting. One would be motivated to do so in order to reduce the time spent by users in attempting to determine the type of such network.

Claim 18: **Fascenda** discloses a secure Wi-Fi communication system and method to enable automatic network roaming as in claim 15 above, and further discloses the connecting devices to be computers (Fig 1). It is inherent that these computers have computer instructions for performing the functions of claim 12 stored thereon.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- d. Turner et al (US 709927) discloses a system and method for wireless network connection.
- e. Yildiz et al (US 6674738) discloses a decoding and detailed analysis of captured frames in IEEE 802.11 wireless LAN.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571)

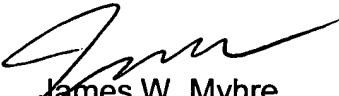
Art Unit: 2112

270-1685. The examiner can normally be reached Monday through Thursday from 7:30 a.m. to 4:30 p.m. and every other Friday from 7:30 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jim W. Myhre, can be reached on (571) 272 6722. The fax phone number for Formal or Official faxes to Technology Center 2100 is (571) 273-3800. Draft or Informal faxes, which will not be entered in the application, may be submitted directly to the examiner at (571) 274-1685.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

FT
January 3, 2007


James W. Myhre
Supervisory Patent Examiner